[19]中华人民共和国国家知识产权局

[51]Int. Cl[7]
H04Q 7/38
H04Q 7/34

[12]发明专利申请公开说明书

[21]申请号 00122497.2

[43]公开日 2001年2月14日

[11]公开号 CN 1283948A

[22]申请日 2000.8.4 [21]申请号 00122497.2
[30]优先权
[32]1999.8.6 [33]US [31]09/369,940
[71]申请人 朗迅科技公司
地址 美国新泽西州
[72]发明人 王 泽 刘春智
帕图尔德哈那·巴布·高勒帕蒂

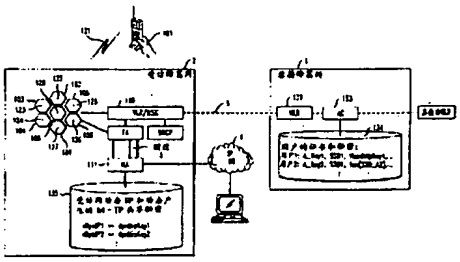
[74]专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 蒋世迅

权利要求书6页 说明书11页 附图页数8页

[54]发明名称 无线通信系统的动态原籍代理系统

[57]摘要

无线通信系统的动态原籍代理系统利用电话信令网和增强型蜂窝验证中心的现 有基础设施以保密方式支持受访无线网或原籍无线网中的动态原籍代理,给漫 游的移动用户台提供分组数据服务。在这些网络中部署验证中心作为蜂窝安全 机构,用于提供蜂窝服务资格检验和防止交换密钥产生的蜂窝欺诈。利用动态 移动IP密钥(DMIPKEY)的附加密钥增强蜂窝安全机构,受访网中的 动态原籍代理利用DMIPKEY鉴别移动用户台请求的移动IP注册。



ISSN1008-4274

知识产权出版社出版

权 利 要 求 书

1. 一种无线通信系统的动态原籍代理系统，通过动态分配原籍无线网和受访无线网之一的原籍代理，给受访无线网中漫游的移动用户台提供分组数据服务，包括：

一个装置，响应于所述移动用户台向所述受访无线网注册分组数据服务和请求分配所述受访无线网和所述原籍无线网之一的动态 IP 地址，把动态 IP 地址的所述请求转发给所述原籍无线网；

一个装置，位于所述原籍无线网的所述验证中心和所述移动用户台，用于以保密方式动态产生所述移动用户台与动态选取的原籍代理之间共享的移动互联网协议共享秘密，能够安全地进行移动性约束更新；

一个装置，在所述受访无线网和所述原籍无线网的所述之一中，和响应于产生和发射所述移动用户台的鉴别信息给所述动态选取的原籍代理，在所述验证中心没有传输所述移动互联网协议共享秘密给所述漫游移动用户台和所述受访无线网的情况下，用于鉴别所述移动用户台请求的移动互联网协议注册。

2. 按照权利要求 1 的动态原籍代理系统，其中所述转发装置包括：

来访者位置寄存器装置，用于通过连接所述原籍无线网和所述受访无线网的电话信令网，发射动态 IP 地址的所述请求给所述原籍无线网的原籍位置寄存器，其中所述请求传输通过所述验证中心。

3. 按照权利要求 2 的动态原籍代理系统，还包括：

一个装置，在所述验证中心，响应于不具有蜂窝鉴别和话音加密算法能力的所述来访者位置寄存器，用于建立动态移动互联网协议共享秘密；

一个装置，用于返回所述产生的动态移动互联网协议共享秘密给所述原籍位置寄存器；

一个装置，用于通过所述电话信令网转发响应消息中所述产生的

动态移动互联网协议共享秘密给所述来访者位置寄存器。

4. 按照权利要求 3 的动态原籍代理系统，其中所述鉴别装置包括:

一个装置，位于所述受访无线网，和响应于所述响应消息中存在所述动态移动互联网协议共享秘密，用于动态选取位于所述受访无线网中的本地原籍代理;

一个装置，用于分配动态 IP 地址给所述移动用户台;

一个装置，用于传播所述移动用户台的分配动态 IP 地址和所述导出移动互联网协议共享秘密给位于所述受访无线网中所述动态选取的原籍代理;

一个装置，把所述动态选取的原籍代理的 IP 地址结合到发射给所述移动用户台的响应消息中。

5. 按照权利要求 4 的动态原籍代理系统，还包括:

一个装置，用于在具有所述增强型蜂窝鉴别和话音加密算法的所述移动用户台中产生所述导出移动互联网协议共享秘密; 和

一个装置，在所述移动用户台中，利用所述动态选取的原籍代理的所述 IP 地址和所述导出移动互联网协议共享秘密，启动移动互联网协议注册。

6. 按照权利要求 2 的动态原籍代理系统，还包括:

一个装置，在所述验证中心，响应于具有增强型蜂窝鉴别和话音加密算法能力的所述来访者位置寄存器，用于产生一个指示，该指示请求所述来访者位置寄存器产生移动互联网协议密钥;

一个装置，返回所述指示给所述原籍位置寄存器;

一个装置，用于通过所述电话信令网转发响应消息中的所述指示给所述来访者位置寄存器。

7. 按照权利要求 6 的动态原籍代理系统，其中所述鉴别装置包括:

一个装置，在所述受访无线网中，和响应于在所述响应消息中存在所述指示，用于动态选取位于所述受访无线网中的本地原籍代理;

一个装置，在所述受访位置寄存器中，用于导出动态移动 IP 秘密；

一个装置，用于分配动态 IP 地址给所述移动用户台；

一个装置，用于传播所述移动用户台的分配动态 IP 地址和所述移动互联网协议共享秘密给位于所述受访无线网中所述动态选取的原籍代理；

一个装置，把所述动态选取的原籍代理的 IP 地址结合到发射给所述移动用户台的响应消息中。

8. 按照权利要求 7 的动态原籍代理系统，还包括：

一个装置，用于在配备所述增强型蜂窝鉴别和话音加密算法的所述移动用户台中产生所述导出移动互联网协议共享秘密；和

一个装置，在所述移动用户台中，利用所述动态选取的原籍代理的所述 IP 地址和所述导出移动互联网协议共享秘密，启动移动互联网协议注册。

9. 按照权利要求 2 的动态原籍代理系统，还包括：

一个装置，在所述鉴别中心，响应于请求分配所述原籍无线网中动态 IP 地址的所述来访者位置寄存器，用于建立动态移动互联网协议共享秘密；

一个装置，用于返回所述产生的动态移动互联网协议共享秘密给所述原籍位置寄存器；

一个装置，用于动态选取位于所述原籍无线网中的本地原籍代理；

一个装置，用于分配动态 IP 地址给所述移动用户台；

一个装置，用于传播所述移动用户台的分配动态 IP 地址和所述移动互联网协议共享秘密给所述原籍无线网中所述动态选取的原籍代理；

一个装置，把所述动态选取的原籍代理的 IP 地址结合到发射给所述移动用户台的响应消息中。

10. 按照权利要求 9 的动态原籍代理系统，还包括：

一个装置，用于在配备所述增强型蜂窝鉴别和话音加密算法的所述移动用户台中产生所述导出移动互联网协议共享秘密；和

一个装置，在所述移动用户台中，利用所述动态选取的原籍代理的所述 IP 地址和所述导出移动互联网协议共享秘密，启动移动互联网协议注册。

11. 一种操作无线通信系统的动态原籍代理系统的方法，通过动态分配原籍无线网和受访无线网之一的原籍代理，给所述受访无线网中的漫游移动用户台提供分组数据服务，包括以下步骤：

响应于所述移动用户台向所述受访无线网注册分组数据服务和请求分配所述受访无线网和所述原籍无线网之一的动态 IP 地址，把动态 IP 地址的所述请求转发给所述原籍无线网；

在所述原籍无线网的所述验证中心和所述移动用户台，用于以保密方式动态产生所述移动用户台与动态选取的原籍代理之间共享的移动互联网协议共享秘密，能够安全地进行移动性约束更新；

在所述受访无线网和所述原籍无线网的所述之一中，响应于产生和发射所述用户台的鉴别信息给所述动态选取的原籍代理，在所述验证中心没有传输所述移动互联网协议共享秘密给所述漫游移动用户台和所述受访无线网的情况下，用于鉴别所述移动用户台请求的移动互联网协议注册。

12. 按照权利要求 1 操作动态原籍代理系统的方法，其中转发步骤包括：

通过连接所述原籍无线网和所述受访无线网的电话信令网，从来访者位置寄存器发射动态 IP 地址的所述请求给所述原籍无线网的原籍位置寄存器，其中所述请求传输通过所述验证中心。

13. 按照权利要求 12 操作动态原籍代理系统的方法，还包括以下步骤：

在所述验证中心，响应于不具有蜂窝鉴别和话音加密算法能力的所述来访者位置寄存器，建立动态移动互联网协议共享秘密；

返回所述产生的动态移动互联网协议共享秘密给所述原籍位置寄存器；

通过所述电话信令网转发响应消息中所述产生的动态移动互联网

协议共享秘密给所述来访者位置寄存器。

14. 按照权利要求 13 操作动态原籍代理系统的方法，其中所述鉴别步骤包括:

在所述受访无线网中，响应于所述响应消息中存在所述动态移动互联网协议共享秘密，动态选取位于所述受访无线网中的本地原籍代理;

分配动态 IP 地址给所述移动用户台;

传播所述移动用户台的分配动态 IP 地址和所述导出移动互联网协议共享秘密给位于所述受访无线网中所述动态选取的原籍代理;

把所述动态选取的原籍代理的 IP 地址附加到发射给所述移动用户台的响应消息中。

15. 按照权利要求 14 操作动态原籍代理系统的方法，还包括以下步骤:

在配备所述增强型蜂窝鉴别和话音加密算法的所述移动用户台中产生所述导出移动互联网协议秘密; 和

在所述移动用户台中，利用所述动态选取的原籍代理的所述 IP 地址和所述导出移动互联网协议共享秘密，启动移动互联网协议注册。

16. 按照权利要求 14 操作动态原籍代理系统的方法，还包括以下步骤:

在所述验证中心，响应于具有增强型蜂窝鉴别和话音加密算法能力的所述来访者位置寄存器，产生一个指示，该指示请求所述来访者位置寄存器产生移动互联网协议密钥;

返回所述指示给所述原籍位置寄存器;

通过所述电话信令网转发响应消息中所述指示给所述来访者位置寄存器。

17. 按照权利要求 13 操作动态原籍代理系统的方法，其中所述鉴别步骤包括:

在所述受访无线网中，和响应于在所述响应消息中存在所述指示，动态选取位于所述受访无线网中的本地原籍代理;

在所述受访位置寄存器中，导出动态移动 IP 秘密；

分配动态 IP 地址给所述移动用户台；

传播所述移动用户台的分配动态 IP 地址和所述移动互联网协议共享秘密给位于所述受访无线网中所述动态选取的原籍代理；

把所述动态选取的原籍代理的 IP 地址结合到发射给所述移动用户台的响应消息中。

18. 按照权利要求 17 操作动态原籍代理系统的方法，还包括以下步骤：

在配备所述增强型蜂窝鉴别和话音加密算法的所述移动用户台中产生所述导出移动互联网协议共享秘密；和

在所述移动用户台中，利用所述动态选取的原籍代理的所述 IP 地址和所述导出移动互联网协议共享秘密，启动移动互联网协议注册。

19. 按照权利要求 18 操作动态原籍代理系统的方法，还包括以下步骤：

在所述鉴别中心，响应于请求分配所述原籍无线网中动态 IP 地址的所述移动用户台，建立动态移动互联网协议秘密；

返回所述产生的动态移动互联网协议秘密给所述原籍位置寄存器；

动态选取位于所述原籍无线网中的本地原籍代理；

分配动态 IP 地址给所述移动用户台；

传播所述移动用户台的分配动态 IP 地址和所述移动互联网协议秘密给所述原籍无线网中所述动态选取的原籍代理；

把所述动态选取的原籍代理的 IP 地址结合到发射给所述移动用户台的响应消息中。

20. 按照权利要求 18 操作动态原籍代理系统的方法，还包括以下步骤：

在配备所述增强型蜂窝鉴别和话音加密算法的所述移动用户台中产生所述导出移动互联网协议秘密；和

在所述移动用户台中，利用所述动态选取的原籍代理的所述 IP 地址和所述导出移动互联网协议共享秘密，启动移动互联网协议注册。

00.03.04

说　　明　　书

无线通信系统的动态原籍代理系统

本发明涉及无线通信系统，具体涉及借助于移动 IP 原籍代理和 IP 地址的动态分配，提供分组数据服务给漫游的移动用户台，其中涉及保密方式下的动态分配。

无线通信系统领域中的一个是问题是，给漫游的移动用户台提供接入分组数据服务，它涉及保密方式下原籍代理和互联网协议地址的动态分配。在无线用户台原籍无线网中提供的这种服务涉及密钥的分布，能使原籍无线通信系统鉴别无线用户台的标识，不管该移动用户台是在原籍无线网或受访无线网中。这些方案中的密钥分布要求广泛利用无线分组数据服务的密钥分布中心。然而，具有这些密钥分布中心的分组数据中央基础设施在今天还不是广泛地使用的，或建造和部署这种基础设施是很昂贵的。没有这种基础设施，不安全通信网上的密钥分布可以泄露这种数据，利用非法得到无线用户台的鉴别数据，能够以偷窃服务的形式犯下通信欺诈罪。

高级分组数据服务是蜂窝通信的 ITU/IMT-2000 要求规定的第三代（3G）无线通信系统的一部分。除了静态互联网协议（IP）地址分配以外，动态互联网协议地址分配是 3G/IMT-2000 系统中所要求的。利用静态 IP 地址分配，移动用户台的静态 IP 地址是固定的，并由原籍无线网分配。当移动用户台离开它的原籍无线网时（漫游），需要在受访无线网与原籍无线网之间建立专用数据通信链路（移动 IP 隧道）。在此情况下，按照标准的 IP 路由选择，目的地为原籍无线网中移动用户台 IP 地址的 IP 分组被路由到原籍无线网。在原籍无线网中利用移动 IP 隧道把目的地为移动用户台静态 IP 地址的 IP 分组改发到漫游移动用户台位于和接受服务的受访无线网。当移动用户台从一个无线网覆盖区运动到另一个无线网覆盖区时，移动 IP 移动性约束更新（mobility binding update）是在原籍无线网中的移动用户台与它的原

籍代理之间完成的。由于移动台的 IP 地址和它的原籍代理 IP 地址是静态的或固定的，移动用户台与原籍代理之间共享的秘密可以编程到移动台和它的原籍代理中，所以，原籍代理可以鉴别移动用户台请求的移动 IP 注册，并在保密方式下完成移动性约束更新。

虽然移动 IP 解决无线网之间分组数据移动性的问题，但是，仍然有几个未解决的问题。第一，经过总是停泊在移动台原籍无线网的移动 IP 隧道，不必要的漫长数据传输路由引入额外的网络传输时间和增加网络资源的使用；诸如 IP 电话（通过 IP 的话音）和 H.323 的实时应用中增大网络传输时间的影响是严重的。第二，随着蜂窝分组数据用户的数目增大到几百万，静态 IP 地址分配不可能按比例增大，这个特征是不可利用的。第三，即使当用户不是激活时，原籍代理仍需要保持固定 IP 地址和对应的移动 IP 秘密之间的变换，该秘密是在移动用户台与它们的原籍代理之间共享的。原籍代理提供电话强度可靠性和可用性的负担可能是压倒性的。

由受访无线网动态分配原籍代理和移动台的 IP 地址避免了不必要的漫长路由，有助于减少网络传输时间和提高网络资源的利用率。它还有助于按比例缩放。由于现在可以在传输中（on the fly）建立原籍代理中的变换项目，激活的移动 IP 项目数就较短。高速缓存代替作主（hosting）和较短的项目有助于减轻原籍代理的负担。例如，可靠性和可用性的要求可以远不如以前那样严格。与此同时，假如移动用户台运动到新的受访无线网，则如图 4 所示，受访无线网 2 内的外籍代理与原籍代理之间的移动 IP 隧道提供必需的移动性管理框架。

这类移动 IP 隧道涉及动态原籍代理，它要求以保密方式动态产生移动用户台与它的动态原籍代理之间共享的移动 IP 秘密，因此，随后的移动性约束更新可以安全地进行。当原籍代理是动态的和由受访无线网选取时，用于以前静态 IP 地址分配情况（预分配静态密钥到移动台中）的简单密钥分布解决方法不再有效。因此，动态原籍代理要求更高级的密钥分布方案以支持受访无线网中移动用户台与动态原籍代理之间建立动态移动 IP 秘密。然而，若移动台与动态原籍代理之间动

态秘密的提供和分布不是在保密方式下进行的，则随后的移动性约束更新是不安全的和容易受到攻击。建造具有公共/专用密钥和必需密钥分布中心以提供所需数据安全性的基础设施成本是昂贵的和难以负担的。此外，利用动态原籍代理要求移动用户台知道选取的动态原籍代理的 IP 地址，而 IP 地址可以是在每次会话的基础上变化的。

上述问题的解决和技术进步的获得是由于无线通信系统中这个动态原籍代理系统，它利用电话信令网和增强型蜂窝验证中心的现有基础设施，以保密方式支持受访无线网或原籍无线网中的动态原籍代理。

电话信令网的例子是 ANSI-41 网，GSM MAP 网或二者的组合，且被认为是相对安全的，因为它们只可以接入到有商业漫游协定的无线服务供应商。电话信令网还提供电话强度可靠性，可用性，和服务质量保证。验证中心部署在这些网络中作为蜂窝安全机构，用于提供蜂窝服务资格检验和防止蜂窝欺诈。特别是，在 ANSI 系统中，鉴别密钥（A_Key）是在移动用户台与它相关的验证中心之间共享的秘密。A_Key 绝不通过空中发射，也不在各个移动交换中心之间发射。共享秘密数据（SSD）密钥时时发生变化，这是验证中心确定为必要的，SSD 密钥是利用蜂窝鉴别和话音加密（CAVE）算法从 A_Key 和与移动用户台相关的其他数据中导出的。验证中心和配备 CAVE 算法的移动用户台都可以利用 CAVE 算法独立地产生共享秘密数据密钥。虽然验证中心可以与服务于移动用户台以获得更有效局部处理的受访无线网共享这个共享秘密数据密钥，但是，共享秘密数据密钥绝不通过空中发射。利用共享秘密数据密钥产生其他的密钥，例如，通过空中用于加密数字信令消息的 SMEKEY 和通过空中用于加密数字话音业务的 VPMASK 密钥。

当共享秘密数据密钥不与受访无线网共享时，SMEKEY 或 VPMASK 或二者可以从验证中心送出到使用它的受访系统。然而，来访者位置寄存器不能从 SMEKEY 或 VPMASK 中导出共享秘密数据密钥。由于配备 CAVE 算法的移动用户台和验证中心可以基于共享秘密数据密钥独立地产生 SMEKEY 和 VPMASK，就不需要通过空中发

射 SMEKEY 或 VPMASK。

利用表示为动态移动 IP 密钥（DMIPKEY）的附加密钥，可以增强这个蜂窝安全机构；受访无线网中的动态原籍代理利用 DMIPKEY 鉴别移动用户台请求的移动 IP 注册。DMIPKEY 可以从共享秘密数据密钥或共享秘密数据（SSD）的部分 A（SSD_A）中导出，因为后者是用于鉴别的目的。有了必需的 CAVE 算法增强，配备 CAVE 算法的移动用户台和它的验证中心可以独立地产生 DMIPKEY。由于移动用户台配备 CAVE 算法，不需要通过空中发射 DMIPKEY。

图 1 以方框图形式表示现有技术典型的整个无线通信系统，其中原籍网中的静态移动 IP 原籍代理在蜂窝分组数据服务中利用移动 IP 隧道服务于具有静态 IP 地址的移动台；

图 2 以流程图形式表示利用 CAVE 算法的现有无线通信系统中现有技术用于鉴别和数据加密的密钥产生过程；

图 3 以流程图形式表示无线通信系统中用于鉴别和数据加密的密钥产生过程，其中这个动态原籍代理是在受访网中实现的；

图 4 以方框图形式表示典型的整个无线通信系统，这个动态原籍代理是在该系统中实现的；

图 5 和 6 以流程图形式表示图 4 系统的两种不同操作方式；

图 7 以方框图形式表示典型的整个无线通信系统，其中这个动态原籍代理是在原籍无线网中实现的；

图 8 以流程图形式表示图 7 系统的操作；

图 9 以流程图形式表示利用 GSM 范例的现有无线通信系统中现有技术用于鉴别和数据加密的密钥产生过程；和

图 10 以流程图形式表示利用 GSM 范例的无线通信系统中用于鉴别和数据加密的密钥产生过程，其中这个动态原籍代理是在受访网中实现的。

有静态移动 IP 原籍代理的无线通信系统

图 1 以方框图形式表示现有技术典型的整个无线通信系统，其中静态移动 IP 原籍代理在蜂窝分组数据服务中利用移动 IP 隧道服务于

具有静态 IP 地址的移动台。在描述公开的本发明中，主要的实体是无线通信装置 101，基站 122-128，以及移动交换中心 110，原籍位置寄存器 131，验证中心 133，外籍代理 136，和原籍代理 111。移动交换中心 110 包括呼叫处理和管理呼叫处理的移动电信控制器。这些实体的主要功能是执行与移动交换中心 110 相关的呼叫处理。原籍代理 111，132 和外籍代理 136 提供分组数据移动性管理功能，它涉及移动 IP 注册鉴别 IP 隧道，如在移动 IP 有关的 RFC（请求注释）中所规定的。包括在无线小区 102-108 中的基站 122-128 利用 RF 信道 121 与无线通信装置 101 通信。RF 信道 121 传送命令消息和数字数据，该数字数据可以代表无线通信装置 101 和远端一方中能清楚表达的话音信号。在 CDMA 系统中，用户移动台至少与一个基站 112 通信。

高级分组数据服务是第三代（3G）无线通信系统的一部分，如在无线通信的 ITU/IMT-2000 要求中所规定的。除了静态互联网协议（IP）地址分配以外，在 3G/IMT-2000 系统中要求动态互联网协议地址分配。在静态 IP 地址分配中，当移动用户台 101 离开它的原籍无线网（在受访无线网 2 中漫游）和移动用户台的固定 IP 地址是由原籍无线网 1 分配时，需要在受访无线网 2 与原籍无线网 1 之间建立数据通信链路（移动 IP 隧道 3）。特别是，移动 IP 隧道 3 把受访无线网 2 的外籍代理 136 与原籍无线网 1 的原籍代理 132 互连。移动 IP 隧道 3 把目的地为移动用户台静态 IP 地址的 IP 分组改发到到漫游移动用户台位于和接受服务的受访无线网 2。

当移动用户台 101 从一个无线网覆盖区运动到另一个无线网覆盖区时，由于移动 IP 注册的结果，移动 IP 移动性约束更新是在移动用户台 101 与它的原籍代理（HA）132 之间完成的。由于移动用户台 101 与原籍代理 132 之间存在预编程的秘密，原籍代理 132 可以鉴别移动用户台 101 请求的移动 IP 注册，因此，移动性约束是安全的。

利用 CAVE 算法的鉴别和加密

图 2 以流程图形式表示现有技术用于鉴别和数据加密的密钥产生过程。电话信令网可以是 ANSI-41 网，GSM MAP 网或二者的组合，

且被认为是相对安全的，因为它们只可以接入到有商业漫游协定的无线服务供应商。在这些网络 1，2 中部署验证中心 133 作为蜂窝安全机构，用于提供蜂窝服务资格检验和防止蜂窝欺诈。特别是，鉴别密钥（A_Key）是移动用户台 101 与它相关的验证中心 133 之间共享的秘密。A_Key 绝不通过空中发射，也不在各个移动交换中心之间发射。共享秘密数据（SSD）密钥时时发生变化，这是验证中心 133 确定为必要的，SSD 密钥是利用 CAVE 算法从 A_Key 和与移动用户台 101 有关的其他数据中导出的。验证中心 133 和配备 CAVE 算法的移动用户台 101 都可以利用 CAVE 算法独立地产生共享秘密数据密钥。虽然验证中心 133 可以与服务于移动用户台 101 以获得更有效处理的受访无线网 2 共享这个共享秘密数据密钥，但是，共享秘密数据密钥绝不通过空中发射。利用共享秘密数据密钥产生其他的密钥，例如，通过空中用于加密数字信令消息的 SMEKEY 和通过空中用于加密数字话音业务的 VPMASK 密钥。

当共享秘密数据密钥不与受访无线网 2 共享时，SMEKEY 或 VPMASK 或二者可以从验证中心 133 送出到使用它的受访无线网 2。然而，来访者位置寄存器 110 不能从 SMEKEY 或 VPMASK 中导出共享秘密数据密钥。由于配备 CAVE 算法的移动用户台 101 和验证中心 133 可以基于共享秘密数据密钥独立地产生 SMEKEY 和 VPMASK，就不需要通过空中发射 SMEKEY 或 VPMASK。

有动态移动 IP 原籍代理的无线通信系统

图 4 以方框图形式表示典型的整个无线通信系统结构，其中受访无线网 2 的动态移动 IP 原籍代理在蜂窝分组数据服务中利用动态 IP 地址。受访无线网 2 的动态 IP 地址分配避免了不必要的漫长路由，有助于减少网络传输时间和提高网络资源的利用率。它还有助于可缩放性。由于现在可以在传输中建立原籍代理 111 数据库 135 中的变换，激活移动 IP 项目数就较短。高速缓存代替作主和较短的项目有助于减轻原籍代理的负担。假如移动用户台 101 运动到新的受访无线网，则受访无线网 2 内外籍代理 136 与原籍代理 111 之间的移动 IP 隧道提供

必需的移动性管理框架。例如，可靠性和可用性的要求可以远不如以前那样严格。

这类移动 IP 隧道涉及动态原籍代理，它要求以保密方式动态产生在移动用户台与它的动态原籍代理之间共享的移动 IP 秘密，因此，随后的移动性约束更新可以安全地进行。当原籍代理是动态的和由受访无线网选取时，用于以前静态 IP 地址分配情况（预分配静态密钥到移动台中）的简单密钥分布解决方法不再有效。因此，动态原籍代理要求更高级的密钥分布方案以支持受访无线网中移动用户台与动态原籍代理之间建立动态移动 IP 秘密。然而，若移动台与动态原籍代理之间动态秘密的提供和分布不是在保密方式下进行的，则随后的移动性约束更新是不安全的和容易受到攻击。建造具有公共/专用密钥和必需密钥分布中心以提供所需数据安全性的基础设施成本是昂贵的和难以负担的。此外，利用动态原籍代理要求移动用户台知道选取的动态原籍代理的 IP 地址，而 IP 地址可以是在每次会话的基础上变化的。

受访无线网中的动态原籍代理

利用表示为 DMIPKEY 动态移动 IP 密钥的附加密钥，可以增强图 2 中所描述的这个蜂窝安全机构；如图 4 所示，受访无线网 2 中的动态原籍代理 111 利用 DMIPKEY 鉴别移动用户台 101 请求的移动 IP 注册。DMIPKEY 可以从共享秘密数据密钥或共享秘密数据的部分 A（SSD_A）中导出，因为后者是用于鉴别的目的。有了必需的 CAVE 算法增强，配备 CAVE 算法的移动用户台 101 和它的验证中心 133 可以独立地产生 DMIPKEY。由于移动用户台 101 配备 CAVE 算法，不需要通过空中发射 DMIPKEY。

图 3 以流程图形式表示无线通信系统中用于鉴别和数据加密的密钥产生过程，其中可以实现这个动态原籍代理，而图 4 以方框图形式表示典型的整个无线通信系统结构，这个动态原籍代理是在该系统中实现的；图 5 和 6 以流程图形式表示图 4 系统的两种不同运行方式。

可以利用 DMIPKEY 以支持受访无线网 2 中的动态原籍代理。动态产生分组数据用户的移动 IP 共享秘密过程是用图 4 验证中心 133 的

数据库 134 中 fun（SSD_A，…）表示。在受访无线网 2 的原籍代理 111 中，产生的密钥通过电话信令网 5 送出，并与分配给移动用户台 101 的动态 IP 地址一起由受访无线网 2 传播。具体地说，如图 5 所示，在步骤 501，漫游的移动用户台 101 向受访无线网 2 注册分组数据服务，并请求受访无线网 2 分配动态 IP 地址。在步骤 502，来访者位置寄存器 110 通过电话信令网 5 发射注册/鉴别请求给蜂窝用户的原籍无线网 1 中原籍位置寄存器 131；在步骤 503，注册/鉴别请求传输通过验证中心 133。在步骤 504，验证中心 133 鉴别该用户。

在步骤 505，若受访无线网 2 的来访者位置寄存器 110 不具有 CAVE 算法能力，或若原籍无线网 1 不与受访无线网 2 共享 SSD，则验证中心 133 利用存储在数据库 134 中移动用户台的 SSD_A 和经 fun（SSD_A）产生密钥的增强型 CAVE 算法，建立表示为 dynMipKey 的动态移动 IP 共享秘密。在步骤 506，验证中心 133 返回产生的 dynMipKey 给原籍位置寄存器 131 作为部分的鉴别响应，和在步骤 507，鉴别响应通过电话信令网 5 转发给受访无线网 2 中的来访者位置寄存器 110。若 dynMipKey 出现在响应消息中，则在步骤 508，来访者位置寄存器 110 提取它。在步骤 509，受访无线网 2 选取本地原籍代理和受访无线网 2 中的动态主配置协议（DHCP）服务器分配表示为 vDynIP 的动态 IP 地址给移动用户台 101，和在步骤 510，移动用户台的分配动态 IP 地址和导出移动 IP 共享秘密 dynMipKey 的信息传播给受访无线网 2 中的原籍代理 111。在步骤 511，原籍代理的 IP 地址结合到发射给移动用户台 101 的响应消息中。在步骤 512，若原籍代理的 IP 地址包含在响应消息中，则基于 SSD_A，配备增强型蜂窝鉴别和话音加密算法的移动用户台 101 产生 dynMipKey。在步骤 513，PPP 的正常 IPCP 阶段开始，在此期间由 DHCP 分配给移动用户台 101 的动态 IP 地址和 DNS IP 地址通过 IPCP 消息交换都提供给移动用户台 101。在步骤 514，利用原籍代理的 IP 地址和产生的 dynMipKey，移动用户台启动移动 IP 注册。若原籍无线网 1 与受访无线网 2 的来访者位置寄存器 110 共享 SSD，如果它配备增强型 CAVE 算法。则可以由来访者位置寄存

器 110 产生 DMIPKEY。因此，DMIPKEY 不需要包含在上述的原籍位置寄存器 131 的鉴别响应消息中。这是以流程图的形式表示在图 6 中，其中图 5 的过程改变成说明这种能力。具体地说，图 6 中的步骤 601-604 与图 5 中的步骤 501-504 完全相同。然而，在步骤 605，若受访无线网 2 的来访者位置寄存器 110 具有增强型 CAVE 算法的能力，和原籍无线网 1 与受访无线网 2 共享 SSD，则验证中心 133 产生一个指示，该指示请求来访者位置寄存器 110 产生移动 IP 共享密钥 dynMipKey。在步骤 606，验证中心 133 返回该指示到原籍位置寄存器 131 作为部分的鉴别响应，在步骤 607，鉴别响应通过电话信令网 5 转发给受访无线网 2 中的来访者位置寄存器 110。若该指示出现在响应消息中，则在步骤 608，利用存储在来访者位置寄存器 110 中移动用户台的 SSD_A 和经 fun（SSD_A）产生密钥的增强型 CAVE 算法，来访者位置寄存器 110 产生表示为 dynMipKey 的移动 IP 共享密钥。在步骤 609，受访无线网 2 选取本地原籍代理和受访无线网 2 中的动态主配置协议（DHCP）服务器分配动态 IP 地址 vDynIP 给移动用户台 101，和在步骤 610，移动用户台的分配动态 IP 地址 vDynIP 和导出移动 IP 共享秘密 dynMipKey 的信息传播给受访无线网 2 中的原籍代理 111.在步骤 611,原籍代理的 IP 地址结合到发射给移动用户台 101 的响应消息中。在步骤 612，若原籍代理的 IP 地址包含在响应消息中，则基于 SSD_A，配备增强型蜂窝鉴别和话音加密算法的移动用户台 101 产生 dynMipKey。在步骤 613，PPP 的正常 IPCP 阶段开始，在此期间由 DHCP 分配给移动用户台 101 的动态 IP 地址和 DNS IP 地址通过 IPCP 消息交换都提供给移动用户台 101。在步骤 614，利用原籍代理的 IP 地址和产生的 dynMipKey，移动用户台启动移动 IP 注册。

原籍无线网中的动态原籍代理

图 7 以方框图形式表示典型的整个无线通信系统，在该系统中实现这个动态原籍代理，而图 8 以流程图形式表示图 7 系统的操作。上述图 4 中的相同机构可以用于这种情况，利用位于原籍无线网 1 中的动态原籍代理 132，原籍无线网 1 分配动态 IP 地址。具体地说，在步

骤 801，漫游的移动用户台 101 向受访无线网 2 注册分组数据服务，并请求原籍无线网 1 分配动态 IP 地址。在步骤 802，来访者位置寄存器 110 通过电话信令网 5 发射注册/鉴别请求给蜂窝用户的原籍无线网 1 中原籍位置寄存器 131；在步骤 803，注册/鉴别请求传输通过验证中心 133。在步骤 804A，验证中心 133 鉴别该用户。在步骤 804B，利用存储在数据库 134 中移动用户台的 SSD_A 数据和经 fun（SSD_A，…）产生密钥的增强型 CAVE 算法，验证中心 133 导出表示为 dynMipKey 的动态移动 IP 共享秘密。在步骤 805，验证中心 133 返回移动 IP 共享秘密给原籍位置寄存器 131 作为部分的鉴别响应。在步骤 806，原籍无线网 1 选取原籍代理和原籍无线网 1 中的动态主配置协议（DHCP）服务器分配表示为 hDynIP 的动态 IP 地址给移动用户台 101，和在步骤 807，移动用户台的分配动态 IP 地址 hDynIP 和导出移动 IP 共享秘密 dynMipKey 的信息传播给原籍无线网 1 中的原籍代理 111。在步骤 808，原籍代理的 IP 地址和动态 IP 地址 hDynIP 通过电话信令网 5 转发给受访无线网 2 中的来访者位置寄存器 110，和在步骤 809，原籍代理的 IP 地址结合到发射给移动用户台 101 的响应消息中。在步骤 810，若原籍代理的 IP 地址包含在响应消息中，则基于 SSD_A，配备增强型 CAVE 算法的移动用户台 101 产生 dynMipKey。在步骤 811，PPP 的正常 IPCP 阶段开始，在此期间由 DHCP 服务器分配给移动用户台 101 的动态 IP 地址和 DNS IP 地址通过 IPCP 消息交换都提供给移动用户台 101。在步骤 812，利用原籍代理的 IP 地址和产生的 dynMipKey，移动用户台启动移动 IP 注册。

具有 GSM 能力的系统

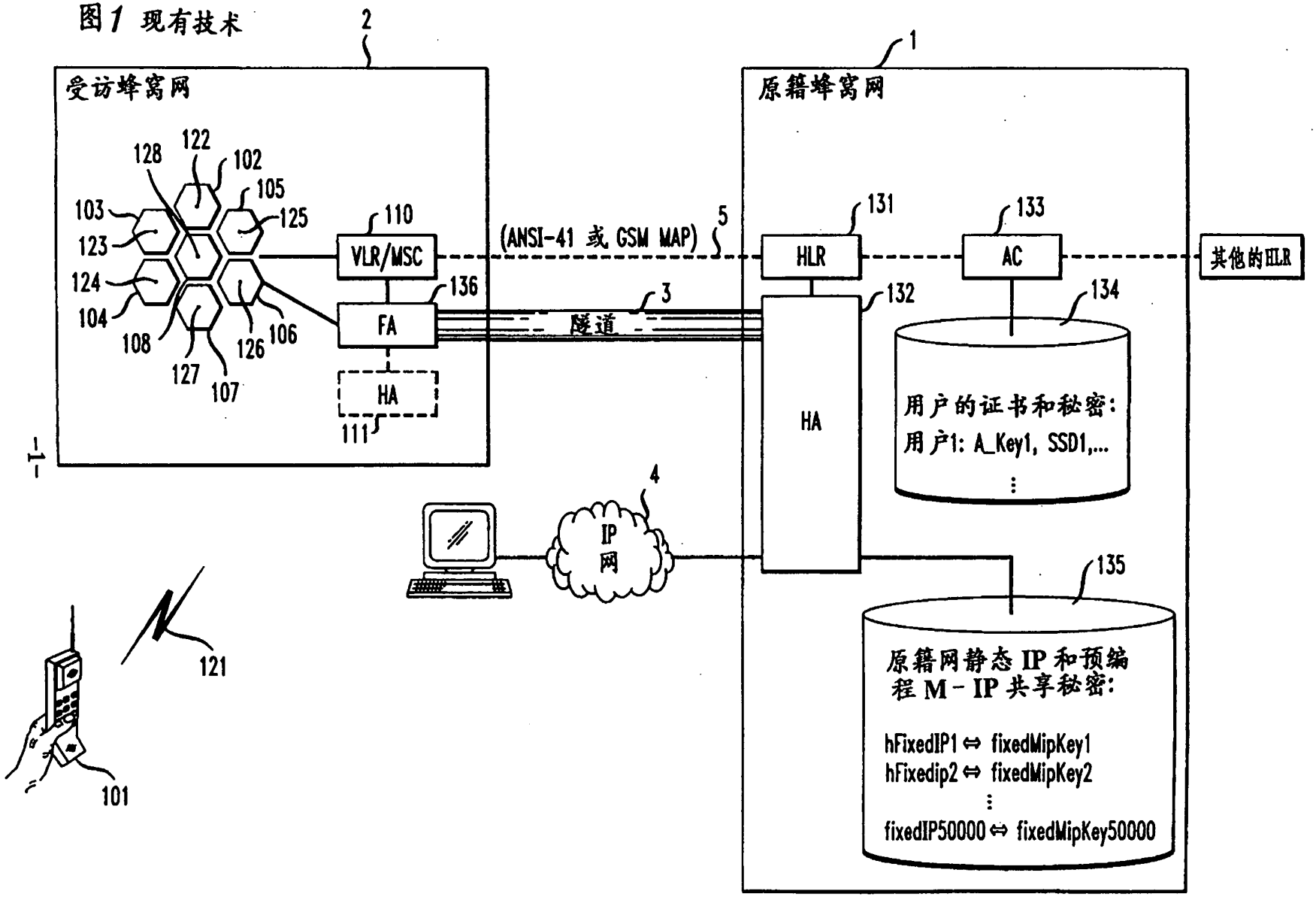
以上的描述集中在利用商品化 CDMA 和 TDMA 网络的增强型 CAVE 算法产生共享秘密。然而，存在一些不利用 CAVE 算法的无线通信系统，其中一个重要的选择是 GSM 网。图 9 以流程图形式表示利用 GSM 范例在现有无线通信系统中现有技术用于鉴别和数据加密的密钥产生过程，而图 10 以流程图形式表示利用 GSM 范例在无线通信系统中用于鉴别和数据加密的密钥产生过程，其中这个动态原籍代

理是在受访网和原籍网中实现的。

GSM 验证中心部署在这些 GSM 网中作为蜂窝安全机构，用于提供蜂窝服务资格检验和防止蜂窝欺诈。具体地说，密码本（Kc）是 GSM 移动用户台与它相关的验证中心之间共享的秘密。具有 GSM 能力的移动用户台和原籍网验证中心能够利用 GSM 鉴别算法（A3）和密码本产生算法（A8）。密码本（Kc）是借助于密码本产生算法 A8 从 Ki 中导出的，用于通过空中加密数字信令消息和通过空中加密数字话音业务。带符号响应（SRES）是借助于 GSM 鉴别算法 A3 从 Ki 中导出的，用于鉴别 GSM 移动用户台。类似于以上描述的增强型 CDMA 和 TDMA 网络，动态移动 IP 密钥（DMIPKEY）可以从带符号响应（SRES）中导出，或由 GSM 验证中心和 GSM 移动用户台从 Ki 中导出，二者都配备增强型 GSM 鉴别算法。然而，与 ANSI-41 验证中心不同，其中来访者位置寄存器可以具有 CAVE 能力，因此，DMIPKEY 可以由来访者位置寄存器产生，而 GSM 验证中心总是通过原籍位置寄存器发射验证中心产生的带符号响应（SRES）和 Ki（在其他的信息中）给来访者位置寄存器。因此，在 GSM 网中，验证中心产生的 DMIPKEY 通过原籍位置寄存器发射给来访者位置寄存器，而来访者位置寄存器不产生 DMIPKEY。

无线通信系统的动态原籍代理系统利用电话信令网和增强型蜂窝验证中心的现有基础设施以保密方式支持受访无线网或原籍无线网中的动态原籍代理。现有的蜂窝安全机构是基于蜂窝鉴别和话音加密（CAVE）算法，通过利用表示为动态移动 IP 密钥（DMIPKEY）的附加密钥，使蜂窝安全机构得到增强，受访无线网或原籍无线网中的动态原籍代理利用 DMIPKEY 安全地鉴别移动用户台请求的移动 IP 注册。

图1 现有技术



说 明 书 附 图

图2

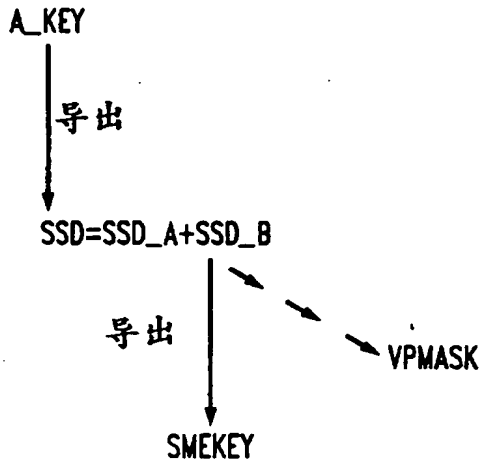

A_KEY
导出
SSD=SSD_A+SSD_B
导出
VPMASK
SMEKEY

图3

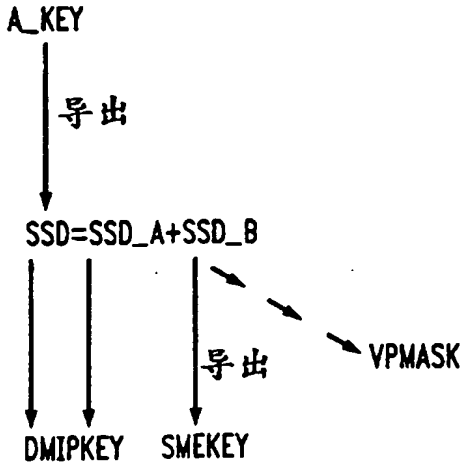

A_KEY
导出
SSD=SSD_A+SSD_B
导出
VPMASK
DMIPKEY
SMEKEY

图 4

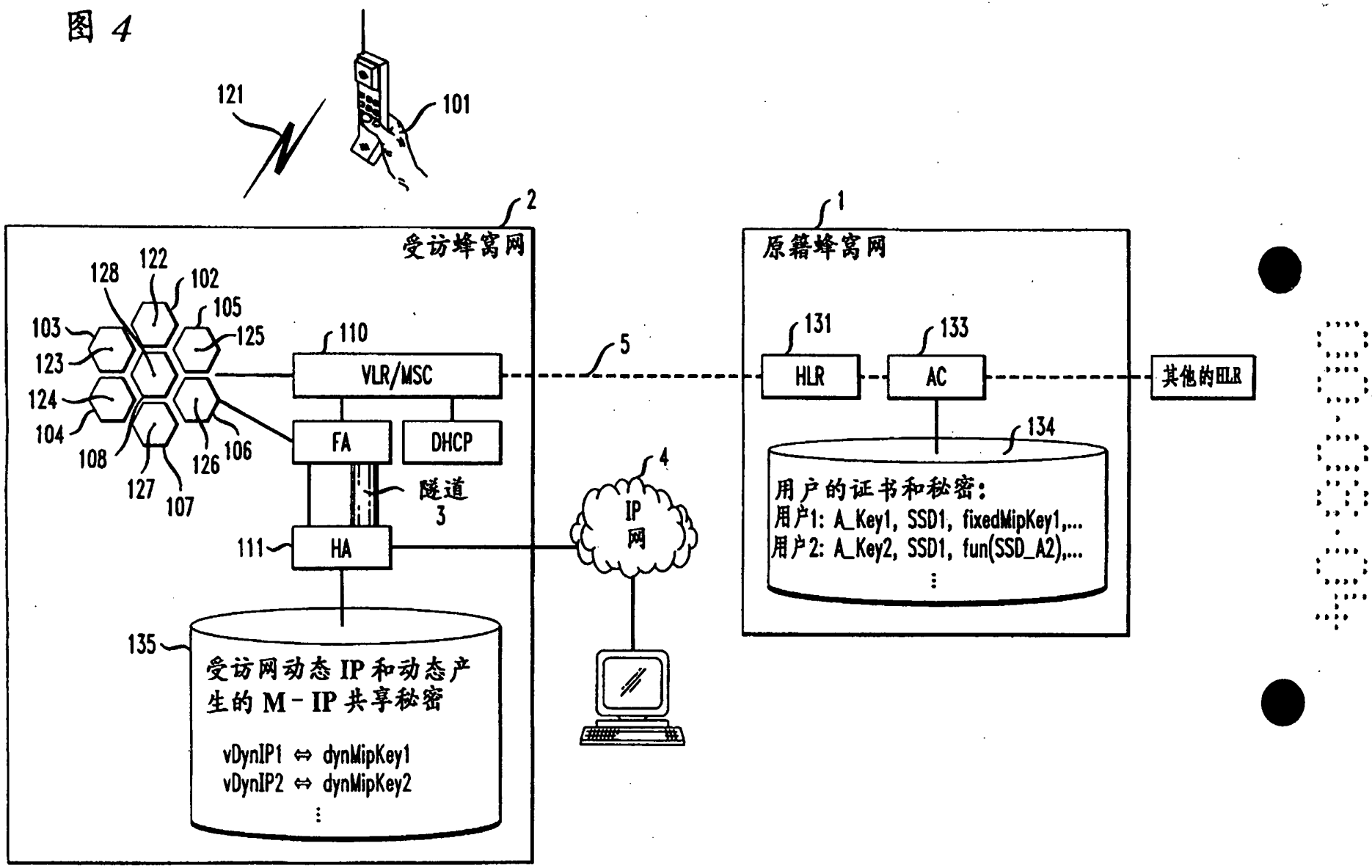

121
101
2
受访蜂窝网
1
原籍蜂窝网
128
122
102
105
103
125
123
124
104
108
126
106
127
107
110
VLR/MSC
5
131
133
HLR
AC
其他的HLR
FA
DHCP
隧道
3
4
IP
网
134
用户的证书和秘密：
用户1: A_Key1, SSD1, fixedMipKey1,...
用户2: A_Key2, SSD1, fun(SSD_A2),...
111
HA
135
受访网动态 IP 和动态产生的 M－IP 共享秘密
vDynIP1 ⇔ dynMipKey1
vDynIP2 ⇔ dynMipKey2

图 5

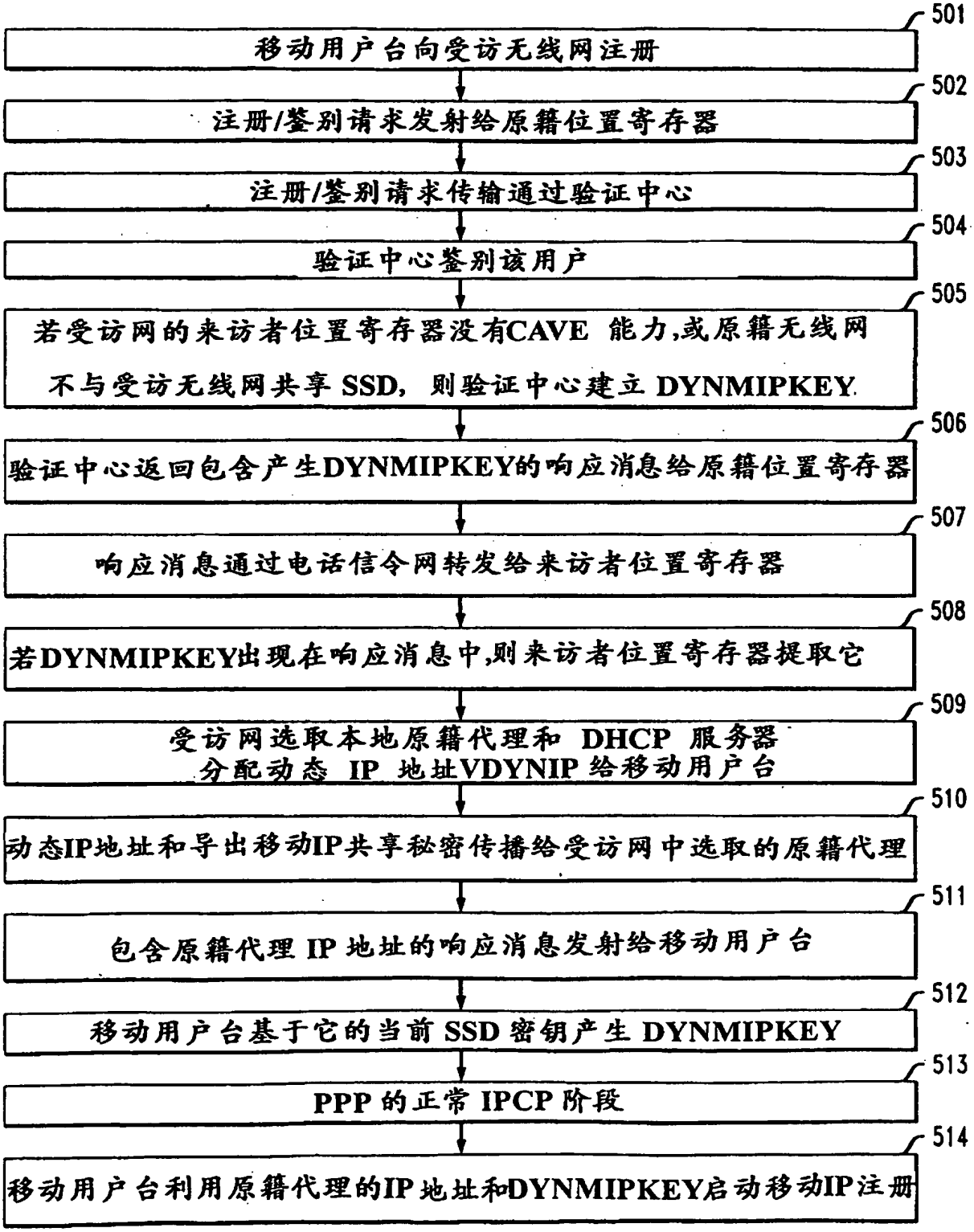

501
移动用户台向受访无线网注册
502
注册/鉴别请求发射给原籍位置寄存器
503
注册/鉴别请求传输通过验证中心
504
验证中心鉴别该用户
505
若受访网的来访者位置寄存器没有CAVE 能力,或原籍无线网不与受访无线网共享 SSD, 则验证中心建立 DYNMIPKEY
506
验证中心返回包含产生DYNMIPKEY的响应消息给原籍位置寄存器
507
响应消息通过电话信令网转发给来访者位置寄存器
508
若DYNMIPKEY出现在响应消息中,则来访者位置寄存器提取它
509
受访网选取本地原籍代理和 DHCP 服务器
分配动态 IP 地址VDYNIP 给移动用户台
510
动态IP地址和导出移动IP共享秘密传播给受访网中选取的原籍代理
511
包含原籍代理 IP 地址的响应消息发射给移动用户台
512
移动用户台基于它的当前 SSD 密钥产生 DYNMIPKEY
513
PPP 的正常 IPCP 阶段
514
移动用户台利用原籍代理的IP地址和DYNMIPKEY启动移动IP注册

图 6

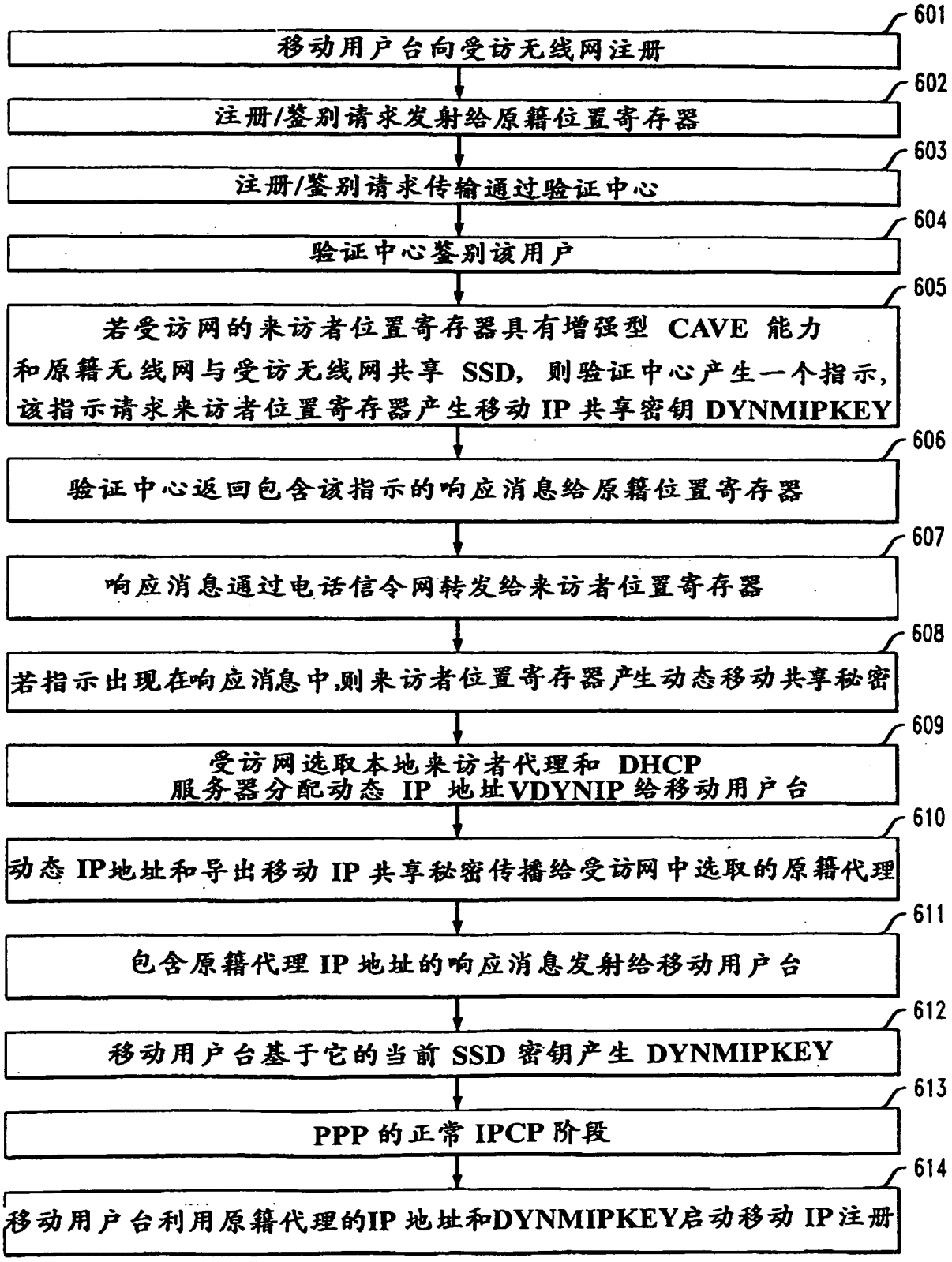
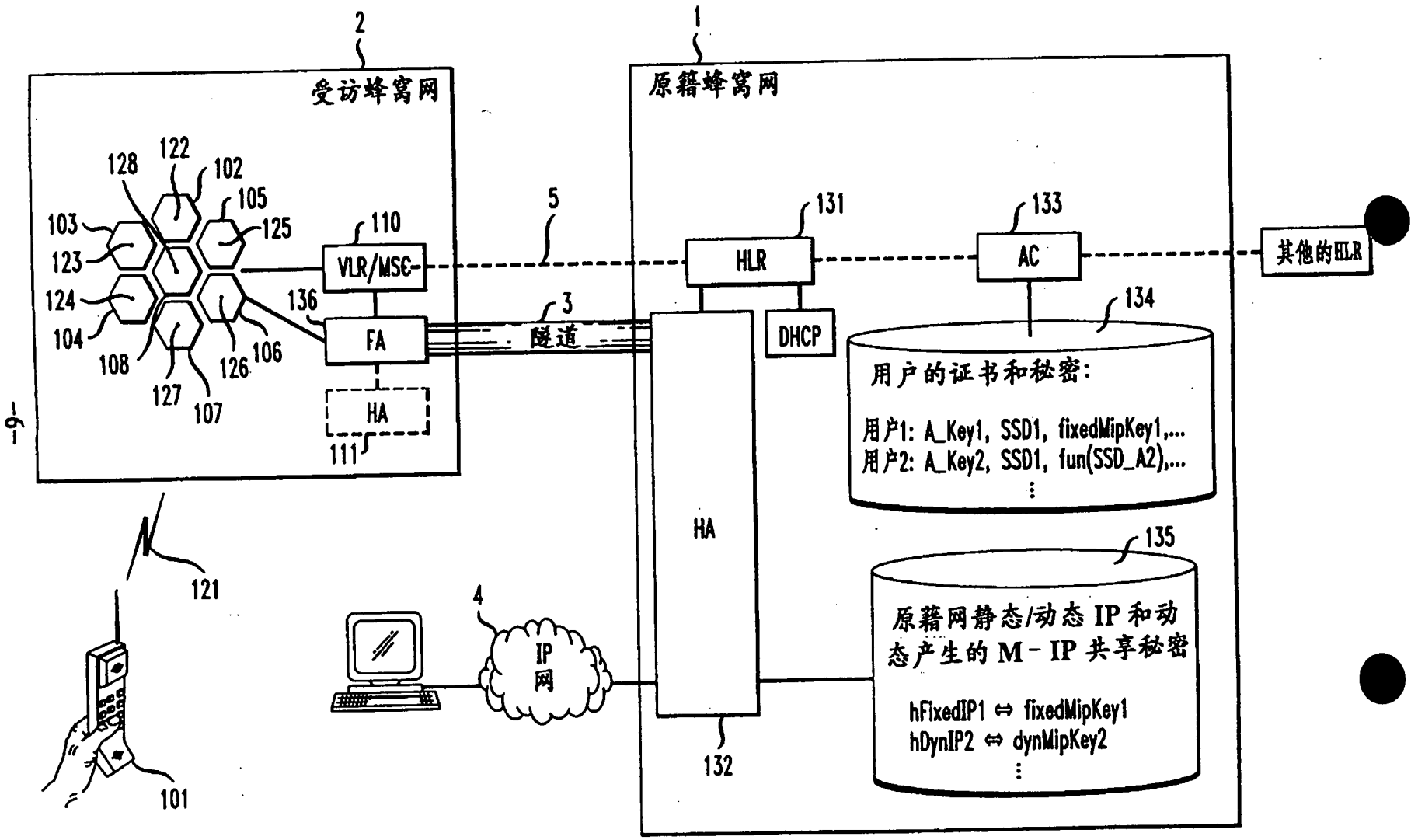

601
移动用户台向受访无线网注册
602
注册/鉴别请求发射给原籍位置寄存器
603
注册/鉴别请求传输通过验证中心
604
验证中心鉴别该用户
605
若受访网的来访者位置寄存器具有增强型 CAVE 能力
和原籍无线网与受访无线网共享 SSD，则验证中心产生一个指示，
该指示请求来访者位置寄存器产生移动 IP 共享密钥 DYNMIPKEY
606
验证中心返回包含该指示的响应消息给原籍位置寄存器
607
响应消息通过电话信令网转发给来访者位置寄存器
608
若指示出现在响应消息中,则来访者位置寄存器产生动态移动共享秘密
609
受访网选取本地来访者代理和 DHCP
服务器分配动态 IP 地址VDYNIP 给移动用户台
610
动态 IP地址和导出移动 IP 共享秘密传播给受访网中选取的原籍代理
611
包含原籍代理 IP 地址的响应消息发射给移动用户台
612
移动用户台基于它的当前 SSD 密钥产生 DYNMIPKEY
613
PPP 的正常 IPCP 阶段
614
移动用户台利用原籍代理的IP 地址和DYNMIPKEY启动移动 IP注册

图 7


2
受访蜂窝网
1
原籍蜂窝网
128
122
102
105
103
125
123
124
104
108
127
107
126
106
110
VLR/MSC
136
FA
HA
111
5
3
隧道
131
HLR
DHCP
133
AC
其他的HLR
134
用户的证书和秘密:
用户1: A_Key1, SSD1, fixedMipKey1,...
用户2: A_Key2, SSD1, fun(SSD_A2),...
HA
132
135
原籍网静态/动态 IP 和动态产生的 M－IP 共享秘密
hFixedIP1 ⇔ fixedMipKey1
hDynIP2 ⇔ dynMipKey2
121
101
4
IP
网

00.08.04

图 8

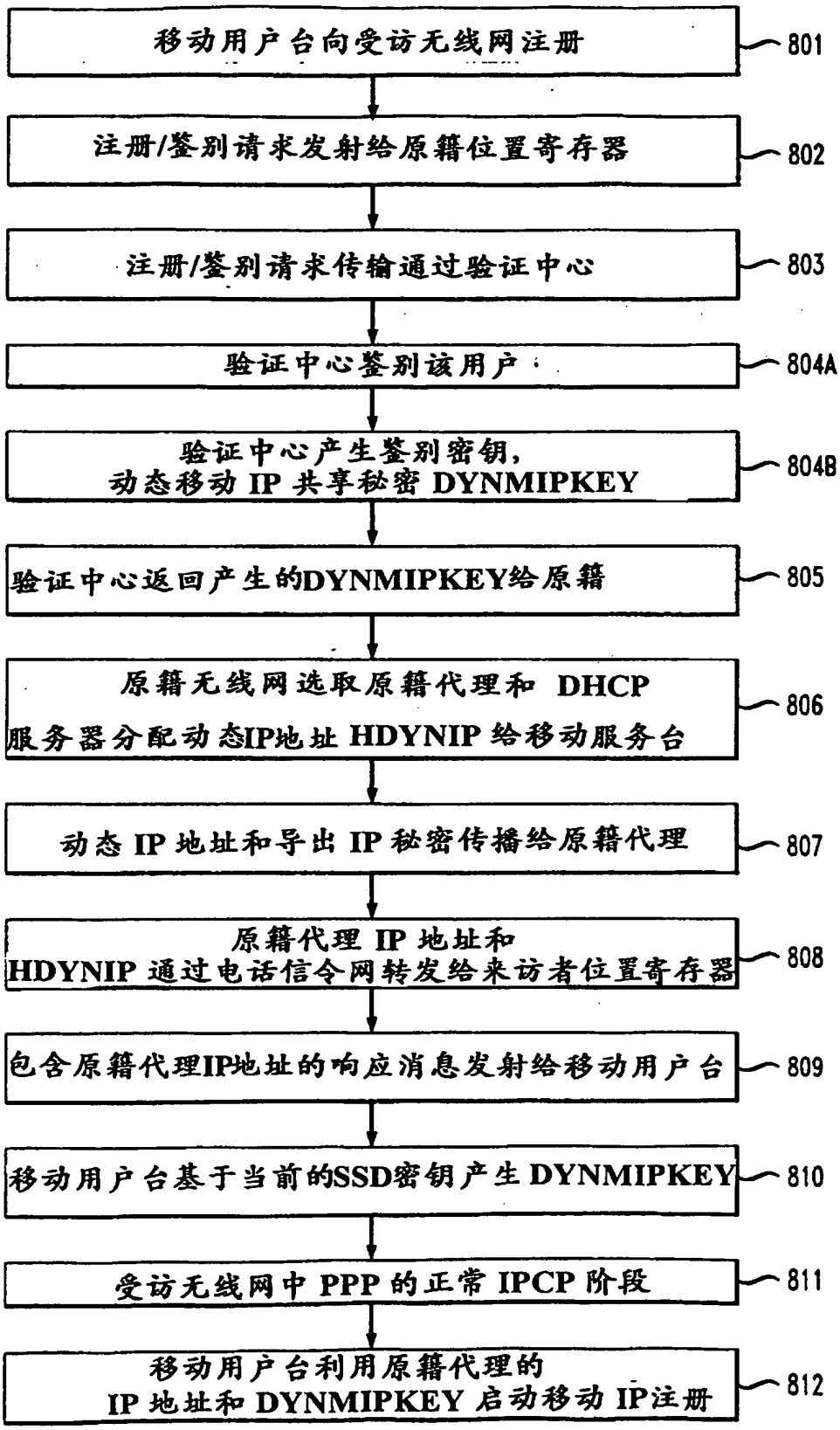

移动用户台向受访无线网注册
801
注册/鉴别请求发射给原籍位置寄存器
802
注册/鉴别请求传输通过验证中心
803
验证中心鉴别该用户
804A
验证中心产生鉴别密钥，
动态移动 IP 共享秘密 DYNMIPKEY
804B
验证中心返回产生的DYNMIPKEY给原籍
805
原籍无线网选取原籍代理和 DHCP
服务器分配动态IP地址 HDYNIP 给移动服务台
806
动态 IP 地址和导出 IP 秘密传播给原籍代理
807
原籍代理 IP 地址和
HDYNIP 通过电话信令网转发给来访者位置寄存器
808
包含原籍代理IP地址的响应消息发射给移动用户台
809
移动用户台基于当前的SSD密钥产生 DYNMIPKEY
810
受访无线网中 PPP 的正常 IPCP 阶段
811
移动用户台利用原籍代理的
IP 地址和 DYNMIPKEY 启动移动 IP注册
812

图 9

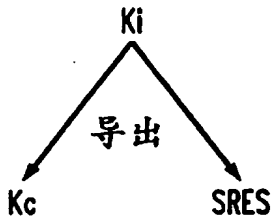


图 10